(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2001 (18.01.2001)

PCT

(10) International Publication Number
WO 01/05090 A1

(51) International Patent Classification[7]: H04L 9/12, 9/26

(21) International Application Number: PCT/EP00/04627

(22) International Filing Date: 19 May 2000 (19.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1012581 13 July 1999 (13.07.1999) NL

(71) Applicant *(for all designated States except US)*: KONINKLIJKE KPN N.V. [NL/NL]; Stationsplein 7, NL-9726 AE Groningen (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MULLER, Frank [NL/NL]; Meerkoetlaan 24, NL-2623 NJ Delft (NL). ROELOFSEN, Gerrit [NL/NL]; Rijndijk 60-A, NL-2331 AH Leiden (NL).

(74) Agent: KRUK, Wiggert, Johan; Koninklijke KPN N.V., P.O. Box 95321, NL-2509 CH The Hague (NL).

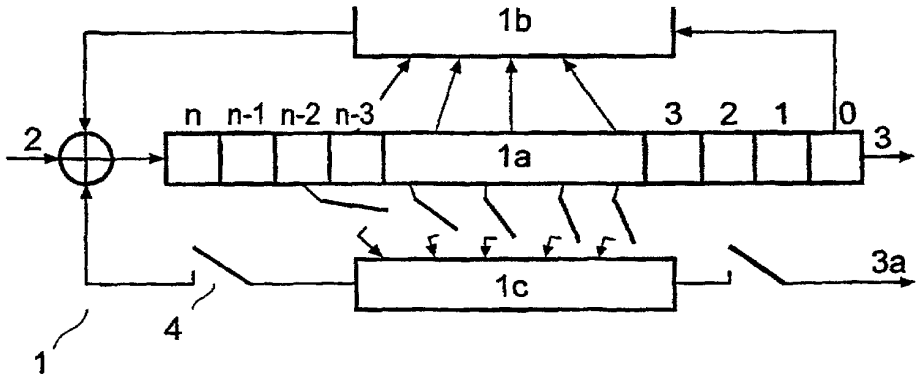
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A METHOD FOR PROTECTING A PORTABLE CARD



(57) Abstract: A method for protecting a portable card, provided with at least a crypto algorithm for enciphering data and/or authenticating the card, against deriving the secret key used from statistical analysis of its information leaking away to the outside world in the event of cryptographic operations, such as power-consumption data, electromagnetic radiation and the like. The card is provided with at least a shift register having a linear and a non-linear feedback funtion for creating cryptographic algorithms. An algorithm is applied to the card, which is constructed in such a manner that the collection of values of recorded leak-information signals is resistant to deriving the secret key from statistical analysis of said values. Advantageously, after the key has been loaded into the shift register, the shift register clocks on, using at least the linear-feedback function. A suitable alternative is loading only the key into the shift register in the event of a fixed content of the shift register.

WO 01/05090 A1